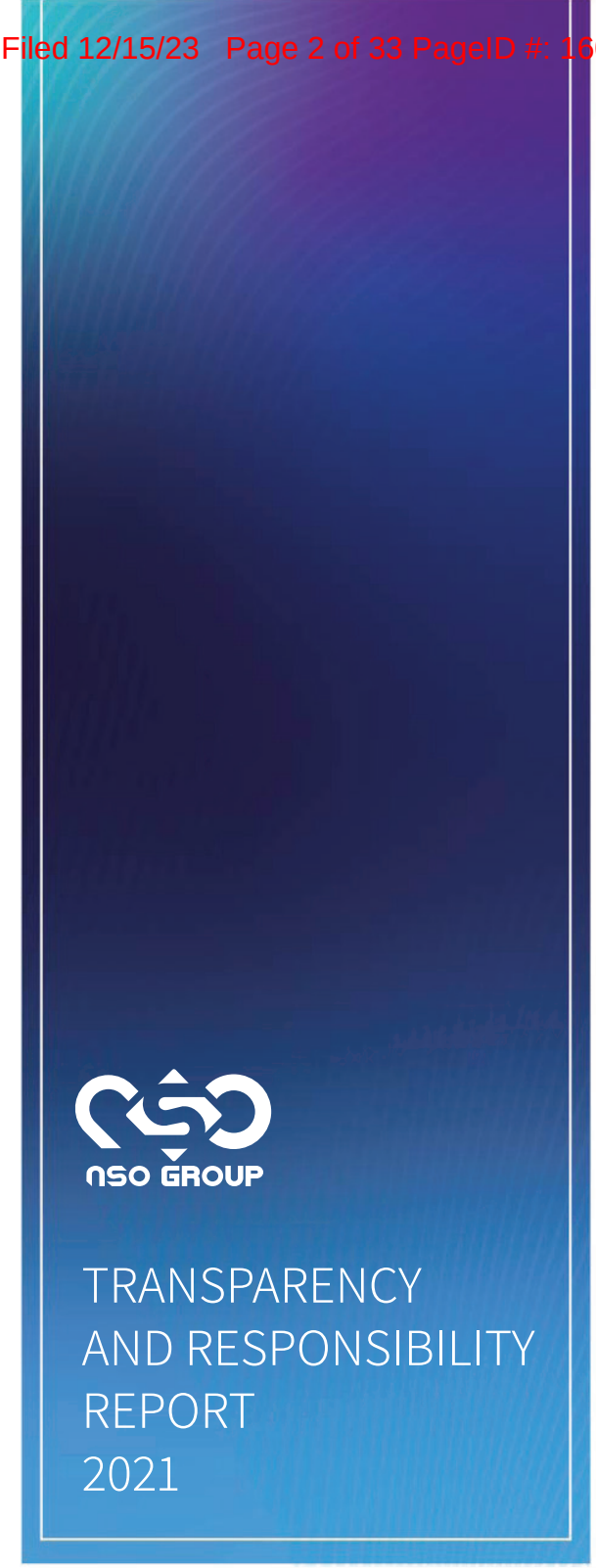
EXHIBIT Q


NSO GROUP
TRANSPARENCY
AND RESPONSIBILITY
REPORT
2021

NSO Group Transparency and Responsibility Report

June 30, 2021

To Interested Parties,

I am honored to sign off on today's public release of the NSO Group's first annual Transparency and Responsibility Report. This is the first of a yearly transparency document that represent an unprecedented step forward into the public conversation space not just for us, but for our industry as a whole. With this document, we not only hope to bring about a deeper, more rounded understanding of who we are and what we do, but we also sincerely hope to inspire others in our sector to follow our example and come forward to explain their own internal ethos and processes. Though there are immense challenges in publishing such a report in an industry that is inherently secretive due to the vital national security considerations of its customers, we have decided nonetheless to "take the plunge" and publish – despite and in spite of these challenges.

Together, as an industry, we must hold ourselves to a higher standard and act with stewardship and transparency, taking into consideration the need for the sensitive balance between states' obligations to ensure public safety and concern for human rights and privacy.

This report has been in the making for a long time. Its final contents are driven by a deep internal desire to take an unflinching, hard-nosed look at how our company has grown in the course of the last decade, how our product offerings are used around the world, and most importantly, how the world has come to perceive the use of our products. The entirety of NSO Group's range of products have been conceived, researched, developed and taken to market with only one simple end-result in mind: the preservation of safety, and the notion that all people should be afforded security and safety in their homes, at work, or out amongst their fellow citizens. We often explain publicly that our products are designed for use by legitimate, vetted, state-administered intelligence and law enforcement organizations. While this remains as true as ever, we must also be assured that all of our sales, and all of the customers who make use of their NSO Group product licenses, are exactly aligned with our ultimate goal: public safety and security. Use of NSO Group products should be methodical, appropriately targeted, limited in reach and scope, and must only be directed by their operators at legitimate criminal or terror group targets.

Still, we acknowledge that on occasion, customers may not meet their obligation as states to protect human rights and adhere to their contractual obligations. This report describes the steps we take in order to try and avoid that from happening in the first place.

This Transparency and Responsibility Report illustrates for the first time, and in deep detail, how NSO Group strives to guarantee that our products are used as intended - safely, effectively and ethically, and it further describes what options are available to us if we find that one of our customers has acted in bad faith, or used one of our tools to target the electronic communications of someone who falls outside the

prescribed target scope. It's simply not enough for us to say that we take instances of misuse seriously. Here, we outline the range of options available to us if this happens, to include completely ending a customer's access to our systems, as a situation may warrant.

That said, we fully recognize that systems and processes must be reviewed and improved regularly, and there are sections of this report that highlight areas in which we want to progress our customer vetting and investigations regimes. It is our sincere intention to learn, and to show, with every subsequent annual report released in the future, that we have further improved our systems of preventing and mitigating misuse of our products by our customers on a worldwide basis.

This is also a great opportunity to thank our investors from Novalpina Capital, our Board and the management of NSO for their commitment and dedication to this unprecedented process.

Lastly, we very much see today's release as a newly added necessity to the complex, ongoing international debate over electronic surveillance. We are opening our own processes to even deeper scrutiny, in an effort to inspire our peers, while also opening new avenues of interaction with our fiercest critics. We remain motivated and candid in our desire to engage with everyone, no matter their position, as we all agree on one thing – the world can and must become a safer place for all.

Sincerely

Shalev Hulio

EXECUTIVE SUMMARY

NSO Group's first annual Transparency and Responsibility Report ("the Report") provides, for the very first time, essential data and insights regarding the company's and responsible business conduct, its governance framework, an outline of our guiding principles, and a detailed account of our ongoing and ever-evolving efforts to help provide products used as they were always intended – to save lives through the prevention of serious crime and acts of terror, as well as through search-and-rescue, data analytics, and other related missions and applications.

This first-of-its-kind Report features comprehensive descriptions of our Compliance and Human Rights policies, and the procedures, processes and practices that we have developed in the course of the last few years to enhance, strengthen and formalize these policies, as well as the day-to-day implementation throughout the entire customer life-cycle. The Report includes the accountings of the structures and goals of each of our internal committees, overviews of our internal and external policies, descriptions of the NSO product marketing and sales life cycle, as well as the remedies we put in place for each scenario.
All of these outlined processes have been devised to honor one central goal: To promote the proper use of our products with integrated steps to mitigate and prevent violations of human rights.
Our products are designed for the sole use of thoroughly vetted and approved governmental agencies charged with maintaining public safety and security.

In addition to detailing the legal and compliance framework that NSO Group has established, the Report also identifies the most salient human rights risks associated with potential customer misuse of our products, and it outlines the concrete steps that the company has taken to mitigate and prevent future instances of misuse, including our human rights due diligence process, in which customer prospects are evaluated prior to any final sales or licensing agreements. The Report also highlights NSO's contractual terms, the company's human rights-focused training programs for employees and customers, and describes how customer engagements can be terminated in the event product misuse is confirmed by our investigative processes.
To date, NSO has rejected over US $300 million in sales opportunities as a result of its human rights review processes.
Additional layers of approval are provided by select government regulatory authorities. NSO Group is closely regulated by export control authorities in the countries from which we export our products: Israel, Bulgaria and Cyprus. The Defense Export Controls Agency ("DECA") of the Israeli Ministry of Defense strictly restricts the licensing of some of our products and it conducts its own analysis of potential customers from a human rights perspective.

Through this first annual Report, we acknowledge the sphere in which we operate requires that some key details, particularly direct identification of our customers or potential customers, remain confidential due to strict contractual and national security considerations. But as the Report explains in detail, there are many steps that can be taken, and that are being taken, to mitigate of risks for human rights violations.
Our work does not stop with the issuance of this first Report. We are fully committed to continue

developing our Compliance and Human Rights policies, and as we will strive over the coming months and years to implement further human rights safeguards and protections, we plan to focus in particular on assessments of the impact of potential misuse of our products in connection with the media and journalists; further analyze recent U.S. guidance and the suggested and adopted changes in E.U. export control laws in comparison with our own processes, and steadfastly support further development of industry standards, rules and regulations for human rights guarantees.

We are proud to be the first company in the cyber intelligence industry to implement policies toward complete alignment with the United Nations Guiding Principles on Business and Human Rights, and we sincerely hope this report helps shed new light on our evolving programs.

1. Overview of NSO and Its Approach

NSO Group was founded in 2010 with one key mission: to make the world a safer place by assisting lawful investigations by state authorities to protect the security and safety of citizens against major crimes and terrorism. Terror organizations, drug cartels, human traffickers, pedophile rings and other criminal syndicates today exploit off-the-shelf encryption capabilities offered by mobile messaging and communications applications. These technologies provide criminals and their networks a safe haven, allowing them to "go dark" and avoid detection, communicating through impenetrable mobile messaging systems. Law enforcement and counterterrorism state agencies around the world have struggled to keep up.

> **Mission**
>
> Help governments protect innocents from terror and crime by providing them with the best intelligence technology of its kind.

Understanding Pegasus

✕ **Myth:** Pegasus is NSO's sole product.
✓ **Fact:** NSO is a technology company with a range of products, including those designed to augment data analytics capabilities by law enforcement and intelligence agencies, improve search and rescue efforts, implement effective counter-measures against incursions by drones.

✕ **Myth:** NSO operates Pegasus, and collects information about the individuals it is used against.
✓ **Fact:** NSO licenses Pegasus to sovereign states and state agencies, does not operate Pegasus, has no visibility into its usage, and does not collect information about customers.

✕ **Myth:** Pegasus is a mass surveillance tool.
✓ **Fact:** Data is collected only from individual, pre-identified suspected criminals and terrorists.

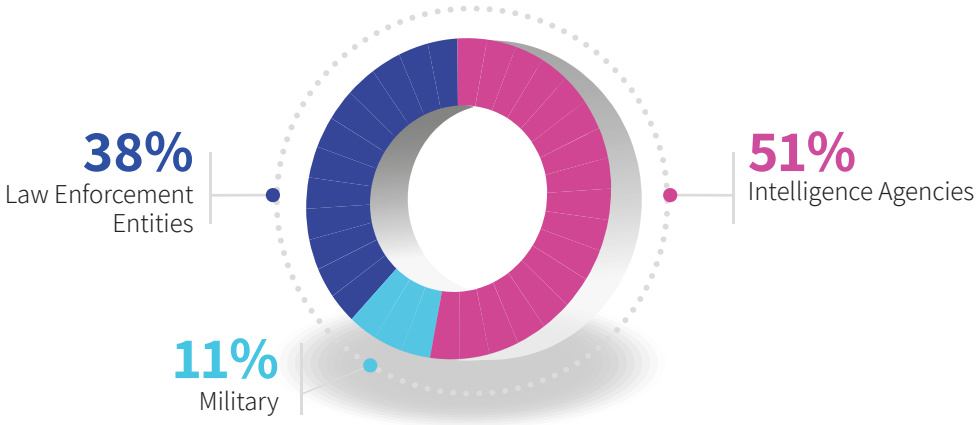
a.Overview of NSO and our Products

As a technology company, NSO Group has developed a variety of products, including those that allow for geolocation of cell phones that is also used for search-and-rescue missions, data analytics systems, and contact tracing to prevent the spread of COVID-19. Our goal is to help states protect their citizens and save lives. Our cutting-edge search-and-rescue products help first responders quickly determine who is missing and locate those individuals, and has helped save lives in multiple catastrophic situations including the Brazil Dam collapse in 2019, Nepal's Earthquake in 2015, Mexico's Earthquake in 2017 and the Tel Aviv parking lot collapse in 2016. Our data analytics tools help law enforcement process massive amounts of data and identify patterns that enable authorities to quickly identify suspects.

It is not a mass surveillance technology, and only collects data from the mobile devices of specific individuals, suspected to be involved in serious crime and terror

Our drone countermeasures products help law enforcement safeguard strategic areas, including airports, stadiums, energy facilities and similar sites, from unwanted surveillance and intrusion. Most recently, we developed an analytics system with advanced mapping capabilities to empower state public health authorities to make informed decisions about mitigation and containment during a pandemic like the COVID-19 outbreak.

60 customers
in
40 countries



NSO's technology has helped …

- …prevent terrorist shooting sprees, car explosions and suicide bombings at transportation hubs, schools, public parks, markets, concert venues, sports arenas and other public areas.
- …break up pedophilia, and sex and drug-trafficking rings.
- …find and rescue kidnapped children.
- …locate survivors trapped under collapsed buildings in the wake of natural disasters or construction failures.
- …map out COVID-19 transmissions and cut off outbreaks.
- …protect airspace against disruptive penetration by drones.

However, we are most well-known for "Pegasus", a technology used by states and state agencies around the world to collect data from the mobile devices of specific suspected major criminals. To be clear, we do not operate this technology. We license it only to the law enforcement and intelligence agencies of sovereign states. Nor do we have any knowledge of the individuals whom states might be investigating, nor the plots they are trying to disrupt, as is otherwise standard amongst our corporate peers. Sovereign states normally do not, will not and should not share this extraordinarily sensitive information.

In addition, while substantial public attention has been drawn to Pegasus, the technology is highly limited in scope. It is used with specific, pre-identified phone numbers, one at a time. In many ways, Pegasus is similar in concept to a traditional wiretap. Instead of listening to specific conversations, it helps law enforcement monitor mobile messaging, offering legitimate law enforcement and intelligence operations personnel a window into the activities of previously identified and targeted criminal actors on an individual basis. Pegasus cannot be used to gather information broadly and does not penetrate computer networks, desktop or laptop operating systems, or data networks. It is not a mass surveillance technology and only collects data from the mobile devices of specific, pre-identified individuals.

Our technology has been used by states to prevent serious crimes and save lives on a massive scale. With the technology, states and state agencies have thwarted numerous major terrorist attacks, captured and brought many pedophiles to justice, broken up criminal organizations and drug trafficking rings and freed kidnapping and human trafficking victims.

Solutions Impact Testimonials:

Pegasus played a pivotal role in combating drug trafficking in our country. Just in the past year, we can attribute over 50 arrests of confirmed drug traffickers that were made, and tons worth of dangerous and prohibited drugs that were caught.

We limit the number of instances in which it can be used, which also reduces the risk it will be used for reasons other than legitimate law enforcement.

b. NSO's Approach to Human Rights

As a company, we are committed to respecting human rights. We work hard to conduct business ethically and responsibly, taking particular care with our most sensitive tools, like Pegasus.

We are committed to the authoritative international standards of the United Nations (UN) Guiding Principles on Business and Human Rights ("UNGPs") and the Organization for Economic Cooperation and Development (OECD) Guidelines for Multinational Enterprises ("OECD Guidelines"), and we honor these commitments with a robust governance framework developed in consultation with leading business and human rights experts, and discussed in detail below. This framework codifies NSO's commitment to ethical business and integrates human rights safeguards into all aspects of our work – from the design to the licensing to the use of our products. While other cyber intelligence technologies have been developed by state agencies and companies in China, Russia, and elsewhere, there is no model to easily replicate or industry standards to help guide us. Nonetheless, to our knowledge, we are the only company in the cyber intelligence industry to have such a thorough governance framework and to have publicly committed to the UNGPs and OECD Guidelines.

We continue to improve our processes, and learn from more insightful analyses, in-depth engagements and investigations over the past year.

As part of our governance framework, we have taken concrete and specific steps, in accordance with international standards, to address and mitigate the human rights risks associated with our products. For example, we license Pegasus only to select approved, verified and authorized states and state agencies, specifically to be used in national security and major law enforcement-driven investigations. We conduct due diligence on those prospective users to assess the risks of misuse. Our standards are higher than the export control requirements of most sovereign states, as well as those of the European Union. We do not license Pegasus to customers where, following our human rights-focused due diligence process, we believe there are inadequate country-level protections in place to confidently prevent misuse, or where the rule of law creates an unduly high risk of misuse. We strictly require that Pegasus is used only where there is a legitimate law enforcement or intelligence-driven reason connected to a specific, pre-identified phone number, and after a process is followed where a state agency decision-maker independent of the user – such as a court - authorizes that use consistent with a written domestic law. Its use against law-abiding citizens is prohibited, and customers, a majority of which are in the EU or OECD, commit that they will use our products responsibly. We limit the number of instances in which it can be used, which also reduces the risk it will be used for reasons other than legitimate law enforcement. Where a customer is accused of misusing our technology, we investigate immediately.

When customers are unable to provide sufficient assurances to remain authorized users of our products, we terminated these relationships.

Where we believe a misuse has occurred, we take immediate action, which has included preventing future use of the system, and try to learn from the situation to prevent it from happening again anywhere else. The Company is very selective with respect to the identity of the countries and customers to which it is willing to sell. Following an in depth review of various compliance concerns the Company has decide

upon a list of over 55 countries to which it has not and will not sell cyber intelligence products to for reasons such as human rights, corruption, and regulatory restrictions. Opportunities from those countries shall not even be brought to the management committee for consideration.Our investigations and engagements with our customers leave us convinced that our products are used appropriately the vast majority of the time. In fact, over the last three years, allegations of misuse amount to less than 0.5% of the instances in which the Pegasus system was used by our customers. Nonetheless, we are acutely aware of the inherent human rights tension associated with our products. The customers for Pegasus are states and state agencies facing the challenge of balancing their duties to protect human rights and individual liberties, while countering major crimes and terrorism. This creates risks for human rights, and the potential for customers to misuse our products. States may be tempted to limit fundamental freedoms to fight terrorism and major criminal activities. In addition, terrorists and criminal enterprises often are based or seek shelter in countries where the rule of law is not always strong, and where the risk our products will be misused by the state agencies charged with investigating them is enhanced. In this context, we believe our framework is thorough and strong, and represents a current best practice in our sector, and we are proud of what we have accomplished to date. But, we also acknowledge that it is not perfect, and we are constantly looking at ways to improve it.

We also strongly advocate that tailored global standards must be developed to assist in guiding our industry.

We therefore have continued to improve our processes, and have learned from more insightful analyses, in-depth engagements and investigations in the course of the past year. We have already implemented some of these improvements and are designing further enhancements based on our findings. These include enhancements to our due diligence, contracting process, protocols regarding auditability, internal customer oversights and approvals, and document retention and destruction. We also have enhanced our processes for uncovering potential misuse and conducting investigations, and have clarified the implications for customers who decline to participate in our investigations. We further have honed our overall risk-tiering, and how we approach customers where we suspect the risks of potential misuse may be elevated. When customers have been unable to provide sufficient assurances to remain authorized users our products, we have terminated these relationships.

This Transparency and Responsibility Report, NSO Group's first and the first of any company in the cyber intelligence industry, is part of our human rights-focused journey. It reflects our activities and learnings over the past year. In providing the report, we are constrained in our ability to transmit information by factors unique to our industry, including rigid confidentiality requirements about our customers and their activities. Our customers are solely authorized intelligence and law enforcement agencies responsible for investigating and, where possible, preventing serious crimes and terrorist acts. To effectively conduct these types of operations, these agencies must operate discreetly in order to (i) infiltrate criminal and terrorist networks to obtain information critical to stopping illegal acts, and (ii) avoid inadvertently giving criminals and terrorists a chance to thwart preventive activities. As a result, our customers mandate strict confidentiality from us and all other service providers in our sector. Our capacity for action is also limited

Solutions Impact Testimonials:

Thanks to NSO Group's cyber intelligence and analytical tools, over 100 terror acts were prevented

by the fact that we do not have visibility into the specific operational uses of our products, unless that access is granted by the customer (as contractually required in the event of an investigation of suspicion that the system has been misused).

Nonetheless, this report provides insights into how we operationalize our mission, and contribute to balance the tensions between the duties of states to protect their populations from physical and criminal threats with their obligations towards freedom of expression, the right to privacy and other human rights. It presents our progress to date and our challenges, risks, and impacts, many of which are unique to our sector. Our ambition is that this report will lead to further engagement with a range of stakeholders resulting in enhancements to our processes and the establishment of widely recognized standards and rules for our industry.

2. NSO's Commitment to Respect Human Rights and Engagement

Our commitment to respect human rights is expressed and embedded in our Human Rights Policy (the HR Policy) discussed in detail below. Developed in 2019, and consistent with the UNGPs and OECD Guidelines, the Policy was adopted by our Board of Directors, and the human rights program is overseen by the Governance, Risk and Compliance Committee of the Board of Directors (the "GRCC"). As the first paragraph of that Policy makes clear:

> **We publicly affirm our unequivocal respect for human rights. The Human Rights Policy is fully endorsed by our senior management and board of directors, who have expressed their full commitment to adhere thereto, is binding on all our employees and stipulates our expectations for all our business partners and customers. We are committed to respecting human rights as enshrined in the International Bill of Human Rights and the principles concerning fundamental rights set out in the International Labor Organizations Declaration on Fundamental Principles and Rights at Work. The United Nations Guiding Principles on Business and Human Rights guide us in fulfilling our obligation to respect human rights throughout business activities.**

While we have expended great effort in developing our human rights program, we strongly believe it can and must continue to improve. We also strongly advocate that tailored global standards must be developed to assist in guiding our industry.

To try to turn those beliefs into actions, we have engaged in a number of affirmative steps. We have assembled a group of human rights advisors to provide NSO Group with guidance regarding its human rights program, provide insights into global standards and trends, and facilitate engagement with academics, civil society organizations, and international institutions.

5 customers we disconnected from the system following an investigation of misuse since 2016

5 customers we discontinued engagements with due to concerns regarding human rights

Estimated loss of revenue following the terminations – over

$100 Million

In particular, we are committed to engagement with civil society organizations to understand the concerns of potentially affected stakeholders, including those whose perspective on our industry and our products differs from our own. To be clear: we will engage in good faith with any credible independent expert, including human rights defenders and others from civil society organizations, representative organizations, companies , or other groups, even if the feedback is critical.

We are committed to engagement with civil society organizations to understand the concerns of potentially affected stakeholders, including those whose perspective on our industry and our products differs from our own.

We believe robust engagement is essential to improve mutual understanding of the risks and challenges associated with balancing the state duty to protect the physical security of its individual populations with the potential misuse of technologies against dissidents, vulnerable populations, and others.

> We will engage in good faith with any civil society organization, representative organization, company, or other group that is willing to engage in good faith, learn about our approach, and provide constructive feedback.

Over the past year, we have engaged with numerous NGOs, receiving useful – and sometimes pointed – feedback and commentary on our human rights program and approach. Many of the recommendations have been integrated into our framework. Examples include sources that we use as part of our due diligence approach, how we might consider enhancing transparency in relation to issues and incidents despite the inherent limitations that exist in our sector, and the integration of additional international standards into our agreements. These suggestions help to strengthen our own processes, and further mitigate risks of misuse and potential adverse human rights impacts by our customers.

We actively support efforts to create standards and mandate further transparency in the cyber intelligence world.

In addition, we actively support efforts to create standards and mandate further transparency in the cyber intelligence world. We have actively promoted engagement around responsible product design and usage in our sector, which balances the need for legitimate law enforcement activities with the risk that state actors misuse cyber intelligence products against journalists, civil society, dissidents and political opponents, and vulnerable populations. We have initiated dialogues with international institutions, in the hope that further engagement among leading companies, state agencies, international institutions and civil society organizations will help establish rules of responsible conduct for our industry. We fully understand, and indeed expect, that some of those rules could require adjustments to our business approach, and even perhaps cause commercial consequences. Still, our steadfast desire is to help develop a global consensus around the appropriate use of cyber intelligence products, and to create confidence among all stakeholders that our products are being used as intended – making the world a safer place.

Throughout 2021 and well beyond, we will continue to pursue and expand these dialogues with the fullest range of stakeholders, including our harshest critics. In these dialogues we have tried to be extremely transparent as evident from our extensive public correspondence with the stakeholders. We acknowledge that some organizations still refuse to engage with us, a position we regret. While that refusal focuses only on the potential negative impacts of our technology and ignores its benefits, by refusing to engage, it precludes us from considering further improvements in light of any insights these organizations might be able to provide. These could include concrete suggestions on corporate due diligence frameworks that they believe could serve as a model for industry standards; examples of contractual provisions that they believe are sound; good practices when end-users commit material breaches, and how those might be incorporated as standards and definitions into our processes and contract terms; or specific limitations or controls to our technology.

> **Solutions Impact Testimonials:**
>
> Our organization made dozens of arrests this year of persons suspected in terror activity, and solved 10 more long standing investigations

Nonetheless, we remain firmly committed to broad stakeholder engagement. We will further customize our approach to meet the needs of each group, and retain an open-door policy for stakeholders willing to engage in good faith, learn about our approach, and provide constructive feedback. We will also continue to pursue engagement with standard-setting international institutions, think tanks and academia, in the hope that progress can be made toward establishing clear and concrete guidance around the design and use of cyber intelligence products that balances individual safety and security with free expression and privacy.

3. Oversight and governance

a. Board Responsibility and the Governance, Risk, and Compliance Committee (GRCC)

Consistent with the UNGPs, oversight of our human rights program starts at the very top of our organization, with our Board of Directors. Our board has adopted various procedures, which we highlight here, for the implementation of our Human Rights Program and periodically discusses human rights issues related to the group's activities.

> Our Governance, Risk and Compliance Committee board reviews potential sales of NSO products, providing recommendations and decisions after an in-depth, risk-based due diligence process including a comprehensive assessment of potential human rights impacts. This newly established committee replaces the Business Ethics Committee. The committee is empowered to reject sales or request investigations into potential misuse.

Our Human Rights Program is governed by the GRCC, whose members are appointed by the Company's Board of Directors. GRCC members select a GRCC chair on an annual basis.

Our external advisors are experienced human rights practitioners and include Cherie Blair leading a team at Omnia Strategy, Gerald Pachoud of Pluto Advisory, partners at Paul Hastings Jonathan Drimmer, Nicola Bonucci and Timothy Dickinson, and Yuval Karniel of Karniel & Co

The GRCC is comprised of NSO's CEO, General Counsel, one independent director, and two other members who are responsible for approving, monitoring and reviewing the Company's policies related to governance, risk and compliance, and overseeing the Company's adherence to Human Rights. As of the date of this report, the current GRCC members are: (1) Gunter Maximilian Schmid (Senior Advisor, Novalpina), who chairs the committee and acts an Independent Advisor, Asher Levy (Executive Chairman, NSO), Stefan Kowski (Founding Partner, Novalpina), Shalev Hulio (CEO, NSO) and Shmuel Sunray (General Counsel). The GRCC Committee's remit includes the Company's Human Rights Program, and the related policies, procedures, and implementation of any remedial measures. The GRCC meets monthly and discusses human rights issues and reviews potential sales at nearly every meeting, in addition to any necessary ad hoc meetings to address emergent issues. The GRCC aims for unanimous decisions facilitated by an in-depth discussion and actions to address any concerns raised by any GRCC member. GRCC resolutions are adopted with a simple majority of the members present.

While NSO management is responsible and accountable for the Company's decisions related to sales, the GRCC has final approval authority for sales identified by our due diligence as being high risk, including decisions based upon adherence to the Human Rights Policy. The GRCC may veto business opportunities in accordance with our Human Rights Due Diligence Procedure. The GRCC also has the authority to delay, reject, or approve the sale subject to additional safeguards or conditions as it deems fit.

Solutions Impact Testimonials:

"NSO's products are used to prevent money laundering and human trafficking. Tools like yours prevent loss of life"

The GRCC charter mandates that both the GRCC and NSO management must agree on the analysis of associated risks, key risk mitigating factors, and risk appetite regarding the sale of products. In certain events, the GRCC may recommend an appropriate approach to the full assembly of NSO's Board, which will make the final determination about how to proceed. The GRCC also has the authority to refer any matter it deems appropriate to the full NSO Board. Moreover, all potential sales where NSO's management, including the General Counsel, does not unanimously agree are referred to the GRCC for approval, which helps prevent the business from overruling legal and compliance. Finally, following the approval of a sale by the GRCC, NSO management must report any material adverse changes to the GRCC, including potential adverse impacts and misuses.

The GRCC also discusses and makes decisions regarding investigations of potential product misuses, such as moving from a preliminary to full review, appointing the lead investigator, and reviewing and closing investigations. The GRCC further reviews and approves new Company policies and procedures, including related to human rights and other compliance-related areas.

The HR Policy sets out NSO's expectations of its customers and business partners, and was created to embed the company's commitment to detect, prevent, and address actual and potential adverse human rights impacts throughout our business and governance systems, and provide for or cooperate in their remediation.

b.Management Committee

The Company's Management Committee comprises the Chief Executive Officer, Chief Product Officer and General Counsel. It meets monthly to discuss human rights issues as part of ongoing business operations. In addition, the Management Committee meets monthly, and in ad hoc meetings, to discuss human rights engagement with stakeholders, including academia and NGOs. The Management Committee also reports its decisions to the GRCC every six months.

c. Day-to-day responsibility and related resources

NSO's Vice President for Compliance, who joined NSO on January 1, 2020, along with the Company's General Counsel, is responsible for day-to-day oversight of the Human Rights Program. NSO Compliance and Legal Teams have significant and varied experience. Specifically, NSO's General Counsel joined NSO on November 1, 2019, and has been General Counsel at large Israeli defense corporations for over three decades, with extensive experience in the field. The Compliance and Legal Teams have regular interactions with the business, operations, and external advisors to incorporate human rights considerations into NSO activities, including interactions with customers and deployment of NSO products. Our external advisors are experienced human rights practitioners and include Cherie Blair leading a team at Omnia Strategy, Gerald Pachoud of Pluto Advisory, legal partners at Paul Hastings (Jonathan Drimmer, Nicola Bonucci and Timothy Dickinson), and Yuval Karniel of Karniel & Co[1].

[1]Cherie Blair QC is the Founder and Chair of Omnia Strategy where she focuses on international arbitration, strategic international legal and advisory work and practices as a barrister. She is a Queen's Counsel with over 40 years' experience as a leading barrister specialising in public international law and human rights.
Gerald Pachoud is the managing partner of Pluto & Associates and advises major companies, international organizations and governments on corporate responsibility. Pachoud previously held various positions in the United Nations and the Swiss administration, and served as the Special Adviser to the Secretary General's Special Representative on business and human rights, Professor John Ruggie, from 2005 to 2011.
Jonathan Drimmer is a partner in the Washington, D.C., office of Paul Hastings LLP. He represents and advises companies, individuals, civil society organizations, and others on issues related to business and human rights and other areas of responsible business conduct. In addition to Paul Hastings, he is a Senior Advisor at BSR, a Strategic Advisor to the Secretariat of the Voluntary Principles on Security and Human Rights, and the North American advisor to the Global Business Initiative for Human Rights.
Timothy L. Dickinson is Senior Counsel in the IWCD practice of Paul Hastings and is currently a Professor from Practice at The University of Michigan Law School, a Director for the International Law Institute's Governance and Anti-Corruption Methods course, and was a founding co-chair of the ABA's International Legal Resource Center, which provides global legal assistance in conjunction with the United Nations Development Programme. Mr. Dickinson also served as the chair of the ABA Section of International Law and Practice and served on the Executive Council of the American Society of International Law where he currently serves as a Counselor and member of the Audit Committee. Mr. Dickinson has over 35 years experience in a number of academic and practice areas, including human rights and international law.
Nicola Bonucci is a Partner in the Global Trade and IWCD practices at Paul Hastings. Previously, Bonucci served as the Director for Legal Affairs for the Organization for Economic Cooperation and Development (OECD) and has been working on Responsible Business Conduct, in particular the Guidelines for Multinational Enterprises, for more than two decades. In advising clients, Mr. Bonucci draws on his international experience with compliance programs, investigations, and anti-corruption issues across various legal systems, as well as his deep knowledge of intergovernmental and multilateral processes.
Yuval Karniel a senior lecturer at the Sammy Ofer School of Communications at IDC where he gives courses on Media Policy, Ethics and Law in the Media, Media and Power, and Commercial Advertising. He also was a member of the board of Israel broadcasting authority (IBA) and the chair of the ethics committee.

As part of day-to-day activities, NSO Compliance and Legal Teams coordinate with Client Executives and Sales managers to review contractual obligations in customer accounts, advise on customer compliance obligations, and conduct investigations arising from whistleblower allegations and other reports of potential product misuse, including those raised by NGOs and the media. These teams play a pivotal role in the oversight of customer activities and investigations of alleged misuse through direct engagement with customers to collect data, inquire about allegations of suspected misuse, and ensure adherence to NSO policies governing human rights. NSO's Legal and Compliance Teams also collaborate to structure agreements to mitigate potential adverse human rights impacts.

Specific attention to protect individuals or groups at elevated levels of risk of arbitrary digital surveillance and communication interception.

The Vice President for Compliance works with external advisors to tailor the Company's Human Rights Program to identify, assess, and manage relevant risks. With input from the business, he evaluates the potential adverse human rights impacts of NSO's long-term strategies, targets, and goals. The Vice President, Compliance, with support from the General Counsel, also reviews engagements and business operations for human rights risks, working to maintain, enhance and implement an effective governance system, encouraging transparency regarding potential human rights risks, and establishing human rights performance targets and outcomes. They are responsible for ensuring and championing a corporate culture that embraces respect for human rights through trainings, roundtables, and promoting engagement with company leadership.

We have an escalating set of responses culminating in the termination of use after a substantiated case of severe misuse, material breach of commitments or a refusal to co-operate in an investigation.

The Compliance Team also utilizes external providers for (i) background reports regarding potential customers and countries from multinational service providers that provide similar services to financial institutions and fortune 500 companies with respect to a wide range of regulatory matters such as Anti-Money Laundering (AML) issues and the Foreign Corrupt Practices Act (FCPA), and (ii) analysis of domestic legal frameworks using internationally recognized law firms.

Solutions Impact Testimonials:

During COVID-19, NSO's tools were essential for the exposure and capture a ring of pedophiles

i. Human Rights Policy Overview

Consistent with UNGP 16, the Board and senior management both have endorsed the Company's Human Rights Policy. The HR Policy was adopted in September 2019 and is binding on all Company employees. The HR Policy sets out NSO's expectations of its customers and business partners, and was created to embed the company's commitment to detect, prevent, and address actual and potential adverse human rights impacts throughout our business and governance systems, and provide for or cooperate in their remediation.

The key aspects of our HR Policy include:

- The integration of human rights due diligence procedures to identify, prevent and mitigate the risks of adverse human rights impacts;
- A thorough evaluation throughout our sales process of the potential for adverse human rights impacts arising from the misuse of NSO products, including the past human rights performance and governance standards of the country involved;
- Contractual obligations requiring our customers to limit the use of our products to the prevention and investigation of serious crimes, including terrorism, and to ensure that the products will not be used to violate human rights;
- Specific attention to protect individuals or groups at elevated levels of risk of arbitrary digital surveillance and communication interception; and
- Periodic review of our human rights program by compliance experts, coupled with a commitment to ongoing dialogue with all relevant stakeholders.
- Cooperation with states in fulfilling their duties to ensure that when abuses occur within their territories, those affected have access to effective remedies.

If an investigation identifies actual or potential adverse impacts, we are proactive in addressing these and mitigating, as appropriate.

Our HR Policy is the foundation for our human rights program and reflects NSO's commitment to respect human rights.

Our HR Policy not only integrates human rights due diligence procedures into our business process, but it provides a framework to train directors, managers, employees, and other relevant stakeholders, outlines our promise to maintain effective grievance mechanisms, and communicates the Company's commitment to evaluating reports of alleged product misuse. Through our HR Policy and the accompanying procedures developed with our team of experts, we have designed a program that seeks to mitigate the risks of misuse of our products, and to respect human rights. As we work to embed the HR Policy within our business, we recognize that this is an ongoing process.

Pursuant to our HR Policy, we also include obligations to respect and protect human rights in our contractual agreements with our business partners and customers. Our standard agreements specifically

Our HR Policy was designed to align NSO's business strategy to our human rights commitments and integrate the Company's human rights due diligence procedures into its business processes, including product development, marketing, sales, delivery, training, technical support, and maintenance.

require our customers to use our products solely for the prevention and investigation of serious crimes (including terrorism) and to ensure that the products will not be used to violate human rights. Our agreements also require our customers to comply fully with all relevant laws and regulations, and any other laws and regulations that are applicable to the use of the products. Our customers are required to notify us of any knowledge they have regarding any misuse or potential misuse of the products that may result in human rights violations. We have an escalating set of responses culminating in the termination of use after a substantiated case of severe misuse, material breach of commitments or a refusal to co-operate in an investigation. Our written agreements are discussed in more detail in section 5.1.

We adopted the HRDD Procedure to further implement the HR Policy and help the Company comply with applicable local laws, international norms and human rights principles in April 2020… paying particular attention to potentially vulnerable groups

We recognize the importance of dialogue with our employees, our business partners, our customers, and external stakeholders. We are continuing to build the awareness and knowledge of our employees regarding human rights, and to encourage individuals to speak up without fear of retribution. As a company, we investigate whenever we become aware of a well-founded report of allegedly unlawful digital surveillance and communication interception, including reports raised by the media and NGOs, which might involve a customer's use of our products. If an investigation identifies actual or potential adverse impacts, we are proactive in addressing these and mitigating, as appropriate. We are committed to promoting the importance of the HR Policy and the effective mitigation of related concerns.

The Company's governance framework and compliance program, discussed below, operationalizes the HR Policy, which is also periodically reviewed, updated, and benchmarked against other leading companies in related sectors. Given the rapid evolution of our sector, and the lack of clearly established precedents or good practices, benchmarking is a particular challenge. Nonetheless, we do seek to learn from peer companies and companies in other sectors, and adjust our processes as we gain further insights.

4. Risks to stakeholders, and NSO Group's Salient Risks

Over the course of the past year, through our legal and human rights-focused analysis of our products and new developments, investigations, engagements with third parties and customers, and review of third-party reports, we have identified the most salient human rights risks associated with our products. These

include:

- The potential misuse of our products against people and groups that act to promote or protect human rights in a peaceful manner ("human rights defenders"). These include: (i) journalists; (ii) members of civil society organizations; (iii) lawyers; and (iv) political parties, candidates and supporters.
- The potential misuse of our products for reasons unrelated to national security or law enforcement, such as in support of litigation or to obtain information that may be embarrassing to individuals.
- The use of our products by unauthorized personnel associated with states and state agencies, which is at odds with our agreements and enhances the risks of negative impacts.
- State use of our technology in a manner inconsistent with human rights norms. For instance, there may not be judicial or other independent approval processes, and when they do exist, we have identified situations where the process or protocols for obtaining approval, standards against which approvals should be judged, and/or requirements for documenting the reasoning associated with granting approvals may not be fully transparent.
- State regulations regarding surveillance that may lack: (i) a definition of the nature of offenses that may legitimately lead to surveillance, and categories of people who may be surveilled; (ii) a limit on the duration of surveillance activities; (iii) a clear procedure to be followed when examining and using information obtained; (iv) precautions when communicating gathered information to other parties; and/ or (v) circumstances in which information may be destroyed.

Solutions Impact Testimonials:

"during 2021 we were able to catch a wanted criminal of over a decade, just two months after starting to using Pegasus"

Some of these risks are reflected in news stories and civil society reports alleging misuses of our products. While the confidential nature of our sector prevents us from confirming the existence of customers in those named countries, we are well aware of the media reports, have a thorough investigation protocol discussed below, and are highly mindful of the severity of the human rights impacts as reported.

These impacts can, and in some cases, we believe have resulted in violations by customers of several fundamental human rights. These include: (i) the right to privacy under the UN Universal Declaration of Human Rights ("UNUDHR") (Art. 12) and the International Covenant on Civil and Political Rights ("ICCPR") (Art. 17); (ii) the right to freedom of expression under the UNUDHR (Art. 19) and ICCPR (Art. 19); and (iii) the right to freedom of assembly under the UNUDHR (Art. 20) and ICCPR (Art. 21). Potential violations of the rights to privacy, freedom of expression and assembly also represent the salient human rights risks associated with customers who misuse our products, as judged from the standpoint of the severity of the impact, the remediability of the impact, how widespread the impact might be, and the likelihood of the impact. We reach that conclusion based on: (i) our own observations and the results of our investigations; (ii) engagement with individuals and groups acting on behalf of potential victims of reported misuses; (iii) dialogue with our human rights advisors, other experts, international institutions, and civil society

organizations; and (iv) a review of public reporting, articles and literature associated with our products and sector. The specific steps to prevent and mitigate human rights impacts associated with those salient risks are detailed in the next section.

There are a wide variety of additional government-driven risks that could flow from our technologies. These could include rights associated with the legal and judicial process, such as freedom from arbitrary arrest and detention and similar abuses (ICCPR Art. 9; UNDHR Art. 3, 9) or improprieties in the legal process (ICCPR Art. 14; UNDHR Art. 10), as well as invasions of freedom of thought, conscience and religion (ICCPR Art. 18; UNDHR Art. 18), restrictions on freedom of movement (ICCPR Art. 12; UNDHR Art. 13), or participation in civic life (UNDHR Art. 21).

5. Operationalizing our Commitments

We implemented our HR Policy and accompanying procedures to help embed our Program within our operations and to help ensure that our customers are using our products in accordance with their human rights obligations and our human rights-related requirements. We have committed ourselves to implementing measures to mitigate risks of adverse impact by embedding the HR Policy and related procedures and extensive controls throughout our business and governance systems.

Our HR Policy was designed to align NSO's business strategy to our human rights commitments and integrate the Company's human rights due diligence procedures into its business processes, including product development, marketing, sales, delivery, training, technical support, and maintenance. The potential for human rights abuses arising from misuse of Company products is evaluated as part of the sales process. This evaluation includes consideration of the specific customer and proposed use, and the past human rights performance and governance standards of the country and specific agency in question, among other factors.

In addition, the Company includes obligations to respect human rights and adhere to human rights norms in its contracts with customers and business partners, and implements an escalating set of mitigations in the event of a customer's failure to adhere to these obligations, up to and including termination of the ability to use Company products. Company products are purposely designed to support effective protection of human rights, including mechanisms to prevent accidental misuse and the ability to suspend or terminate in the event of misuse.

We place great primacy on the due diligence review process and use and enforcement of strong contractual terms, aligned with the UNGPs. But we are aware that due diligence, and even strong contractual provisions, are no guarantee that our products in every instance will be used consistently with responsible business conduct. Those concerns are heightened because we are unable to monitor immediate use, and have not yet determined whether there could be a technological solution to prevent customers from targeting vulnerable populations. We compensate through robust contractual terms that seek to institute processes aligned with international standards, and an enhanced review process aimed at screening out customers where the rule of law is weak, local laws do not meet international norms,

or customers are unable or unwilling to provide sufficient assurances. We also continue to engage with a range of stakeholders to try to upgrade our mechanisms and identify others to mitigate the risks of adverse impacts, consistent with the guidance of the UNGPs to continuously improve our human rights program. Our approach is consistent with the approach taken in similar fields where there is limited visibility into how a customer might use a company's product, such as the defense industry.

i. The Human Rights Due Diligence Procedure

We adopted the Human Rights Due Diligence Procedure (the "HRDD Procedure") to further implement the HR Policy and help the Company comply with applicable local laws, international norms and human rights principles, in April 2020. The HRDD Procedure requires the assessment of the potential human rights impact prior to the sale of our products to each customer, paying particular attention to potentially vulnerable groups. We believe our process is best practice and compares favorably with the larger defense industry.

We designed our multi-step HRDD Procedure to help ensure that the Company's actions are consistent with our HR Policy when engaging customers or entering into new territories. The HRDD Procedure requires that prior to engaging in a business relationship, NSO conducts a comprehensive human rights due diligence review of the potential opportunity and the prospective customer. The HRDD Procedure involves stakeholders from the business, Legal, Compliance, and other key departments, and integrates NSO's commitment to identify, prevent, and mitigate risks of adverse impact into the sales process.

The HRDD Procedure encompasses several components: (i) the initial risk assessment, (ii) due diligence, (iii) risk classification, (iv) review and approval, and (v) additional mitigation, where warranted. These procedures were created to identify, prevent, and mitigate the risks of adverse human rights impacts. In addition to this vetting process for specific, potential sales, the HRDD Procedure also requires the Company to review and approve all elevated risk countries where the Company has not previously had marketing opportunities, prior to engaging in any marketing activities. NSO, through these procedures, seeks to interweave its human rights processes into all functions including product development, marketing, sales, and delivery. This process was designed to support the effective governance of product use in accordance with human rights norms.

As part of an effort to interweave the HRDD Procedure into the company's DNA, NSO involves internal stakeholders from: (1) the **Compliance Team** who determines the initial level for due diligence and administers the process; (2) the **General Counsel** who provides the final risk classification and participates in the Management Committee; (3) **the Business** (e.g., sales, training, and technical support teams) who identifies potential customers to gather relevant information for the due diligence process and conducts oversight on post-sales activities; (4) the **Management Committee** who reviews, approves, or declines all customer engagements; and (5) the **GRCC**, who reviews and has a veto right on high risk customer engagements.

NSO has rejected over US $300M in opportunities as a result of its review process.

15% **of potential new opportunities for Pegasus were rejected for human rights concerns in the past year**

NSO performs extensive due diligence on potential customers. From May 2020 through April 2021, approximately 15% of potential new opportunities for Pegasus were rejected for human rights concerns that could not be resolved. In addition, during this same period, approximately half of our potential opportunities were in connection with the lowest risk countries, with more than half of the revenue from new opportunities from low and moderate risk countries. (Risk levels are discussed in the following sections.) Of the potential opportunities, about half – all in connection with countries receiving the lowest risk rankings – were approved without the need for any additional mitigating measures. Every country with moderate or elevated risk rankings were either deferred, rejected, or approved subject to additional mitigating conditions. These include opportunities for maintenance renewal, new business, and upsell for existing customers. In certain instances, in high-risk regions, NSO has either rejected certain opportunities (e.g., in APAC and the Middle East) or deferred opportunities (e.g., Africa).

Initial Risk Assessment

As part of the review required by the HRDD Procedure, when new customers or marketing opportunities are identified, and the Sales team has not already determined that the potential customer or country presents an unduly high risk, the business submits an application to onboard the new customer or country to the Compliance Team. NSO's Compliance Team then conducts an initial risk assessment to evaluate the human rights-related risks. The initial risk assessment is a two-part evaluation of the country and opportunity.

The country evaluation uses external and widely recognized sources focused on: (i) human rights and freedom of speech allowances in the country; (ii) strength of the country's rule of law and political stability; and (iii) perception of corruption in the country to provide insight into the relative strengths of the specific country's protection of human rights. The underlying sources include the Economist Intelligence Unit, Fund for Peace, Vision of Humanity, Freedom House, Transparency International, the

Initial Risk Assessment Considerations

Product type (low risk, moderate risk, high risk)
End-user type and mission
Concurrent mobile numbers in question
Duration of proposed agreement or relationship
Export control laws and regulations, including embargoes and sanctions
Status relevant to international treaties or conventions

World Bank Worldwide Governance Indicators, Trace International, and CIVICUS, which are reviewed and may be updated annually. This analysis results in a numerical score for each country.
Once a country score is assigned, NSO's Compliance Team evaluates the relative risks related to the

opportunity, considering, amongst other factors, the degree to which the specific product(s) could adversely impinge upon the human rights of targeted individuals, the degree to which there is a perceived potential adverse human rights impact, reputational risks, where the product(s) would be use, the relative authority and governance of the customer organization, and other factors, to assign the Opportunity Classification. The opportunity evaluation must include review of the product type and capabilities, customer organization type and mission, and proposed duration of relationship. Using the factors noted above, the Vice President for Compliance will classify opportunities into categories A, B, C, or D, with D being the highest risk.

Initial Risk Classification

The Compliance Team will designate the Initial Risk Classification based on both the Country and the Opportunity scores. These scores will then fall into one of the following categories: (i) low-risk; (ii) moderate-risk; (iii) high-risk; or (iv) no engagement, as described in the following chart.
The HRDD Procedure gives the Compliance Team the authority to adjust the risk score based on the totality of the risks presented and/or historic or other considerations. Once the initial risk assessment

Country Score	A	B	C	D
Above 60	Low	Low	Moderate	NO GO
45-60	Low	Moderate	Elevated	
25-45	Moderate	Moderate	Elevated	
Below 25 and	Elevated	Elevated	Elevated	
Above 20	Presumptively No Go			

is complete, the Vice President for Compliance assigns a risk ranking: high, moderate or low. The Compliance Team then conducts the due diligence review based on the assigned risk level.

Due Diligence Requirements

This due diligence process relies on information gathered from a number of sources, including publicly available sources, the customer, Company employees, partners, and external consultants or investigative firms, when appropriate, and includes:

- Denied parties checks
- Results of media searches in English and local language
- Information from NSO employees
- Information about the domestic legal framework
- Information from the customer
- Input from relevant government authorities
- Reports from external risk and investigation firms

The following chart summarizes the due diligence requirements for each risk classification:

	Risk/Source	Low	Moderate	High
Open Source Intelligence	Results of internal adverse media country and End-User overview research	✓		
	External risk and investigation firm, report to include publicly available information and adverse media country and End-User overview, human rights and foreign policy		Level 1	Level 2
Human Intelligence - questionnaires	Sales Manager	✓	✓	✓
	Activity reports – Onsite and Client Executives [N/A for renewals]	✓	✓	✓
	Support [N/A for new End-User]		✓	✓
	Partner	✓	✓	✓
	Investigation firms		Level 1	Level 2
	Government input (strategy)			✓
Legal Framework	Publicly available information about local laws and legal framework		✓	
	Local legal opinion			✓
	Export Control (E.U., U.S., IL)		Level 1	Level 2
	SDN / Embargoed Countries	Level 1	Level 2	Level 2
	End User questionnaires/interviews			✓

Final Risk Classification, Review and Approval

Once the Compliance Team has completed the procedures outlined above and prepares a memorandum summarizing the review, findings and any proposed mitigation strategies, the General Counsel reviews and determines the final risk classification. Following the General Counsel's risk classification and completion of any additional required due diligence requested by the General Counsel, the Management Committee reviews and has final approval of moderate and high-risk marketing opportunities (new countries without specific customer opportunities) and all specific customer engagements. The GRCC reviews and has final approval in three circumstances: for all high-risk customer engagements; where the Management Committee approval was not unanimous; and where the Management Committee

decided the sale requires the GRCC's attention. The Compliance Team may approve requests to undertake marketing activities in new low risk countries where specific customer opportunities have not been identified. In addition, the Management Committee provides a report describing all opportunities reviewed, including the outcome, to the GRCC every six months.

Contractual Requirements

NSO requires, at a minimum, human rights compliance clauses in all customer agreements, with additional human rights-related assurances required based on identified risks or mitigation measures. The Company's standard contractual agreements with both business partners and customers include obligations that require compliance with all applicable laws and regulations, including laws and regulations governing the use of our products, and international human rights norms, as described at Annex 1. NSO requires that customers and their employees must comply with(i) applicable domestic laws and regulations, (ii) have received and understand NSO's Human Rights Policy, and (iii) shall respect human rights in using the system, including the rights to privacy and freedom of expression (ICCPR 17 and 19). Our customers also warrant that they will "not target individuals or groups because of their race, color, sex, language, religion, political or other opinions, national or social origin, property, birth or other status or their otherwise lawful exercise or defense of Human Rights."

NSO requires, at a minimum, human rights compliance clauses in all customer agreements, with additional human rights-related assurances required based on identified risks or mitigation measures.

As part of the contractual agreement, customers must also commit to only use NSO's systems for legitimate and lawful prevention and the investigation of serious crimes and terrorism. Where not clearly defined under domestic law, or where domestic law is not consistent with international norms, we include definitions of specific crimes and terrorism-related activitoes – based on definitions in international instruments - for which our investigative products may be used.

Customers must also commit to only use NSO's systems for legitimate and lawful prevention and the investigation of serious crimes and terrorism

Further, our customers are required to provide timely notice of any knowledge they may have regarding suspected misuse that may result in a human rights violation, and to cooperate with NSO investigations regarding allegations of human rights violations. Our standard agreements also provide that we may suspend or terminate use of our products for human rights-related misuse of our products. For moderate or high-risk customers, additional risk mitigation measures may be put in place as needed, including full termination of an agreement, enhanced training or contract clauses, certifications, or additional measures.

Ongoing Oversight

All customers are subject to ongoing oversight for compliance with the terms of their agreements and our HR Policy. Effective monitoring of customer activity is a significant challenge, since we do not have immediate insight into the use of our products. Moreover, as legitimate law enforcement agencies with a mission of protecting against terrorism and serious crime, customers operate with strict confidentiality requirements, including where required by law and/or judicial or customer procedures, and are reluctant to share information to prevent inadvertently compromising security and law enforcement activities. Despite these challenges, we regularly engage with customers to discuss human rights and compliance with the terms of our agreements. We also review public information sources for reports that may suggest potential misuse, and are always seeking additional ways to improve our oversight approach. In addition, we limit the specific crimes in respect of which – and the geographic scope within which – our products may be used, along with the duration of our agreements, where appropriate, in order to ensure that the Company is able to regularly review the appropriateness of each relationship.

ii. Grievance Policies

NSO encourages both internal and external stakeholders to raise concerns of misconduct. The Company's grievance mechanisms allow both confidential and anonymous reporting. However, we encourage whistleblowers to interact directly with an assigned team of discreet investigators, including by providing information that may help substantiate allegations. NSO takes all efforts to keep whistleblower information confidential, where appropriate. Our policies, for both internal and external reports, also reflect the Company's commitment to protect whistleblowers from any unfair or detrimental treatment.

The Internal Whistleblower Policy, adopted in September 2019, encourages openness and support for whistleblowers who raise concerns in good faith, and provides protection for whistleblowers from detrimental treatment as a result of raising genuine concerns. This Internal Policy applies to all employees, consultants, officers, and directors and provides a grievance mechanism to raise concerns to the NSO's most senior management -- including the senior management, General Counsel, and the Vice President for Compliance -- through an anonymous, dedicated email account. Though anonymous reporting is supported, interaction with investigators is encouraged, which allows for a more thorough investigation of all key facts. Investigators are required to evaluate all reports, investigate where there is sufficient information, and conduct extensive analysis and review of credible information.

Similarly, the External Whistleblower Policy, adopted in September 2019, encourages transparency by allowing any external person or body, including contractors, employees, partners, officers, and directors, as well as potentially affected individuals, to report a grievance through a confidential email account, which is reviewed by the Vice President for Compliance. This Policy also encourages interaction with investigators, but provides similar safeguards for whistleblowers.
Once the Company receives a report from a whistleblower or otherwise identifies a concern, including through media or NGO reports, NSO will conduct an investigation using the framework described in the Product Misuse Investigation Procedure. This Procedure involves a preliminary review to determine whether there is sufficient information to identify a potential product misuse, including whether the

allegation is technically feasible. If the Compliance Team determines that a credible claim has been raised, the Management Committee will appoint an investigation team that will conduct an evaluation, including discussions with the customer, collection of additional information, analyzing applicable information, and determining next steps, which may include suspension or termination.

In 2020, NSO conducted 12 product misuse investigations and preliminary reviews, all but one following reports from external whistleblowers or media and NGO reports. Aggregated results of these investigations are discussed in the following section.

2020 INVESTIGATION OF ALLEGED PRODUCT MISUSE

In 2020, following allegations of suspected misuse by a customer, NSO conducted an examination into the customer's deployment of NSO products. This investigation included several meetings with the customer, including top officials at the agency, review of local law by a well-respected law firm in-country, and analysis and determination that NSO products were being used within the terms and agreements set forth by the Company, including the human rights obligations.

It is strict NSO Group policy that employees, consultants, officers, and directors must not threaten or retaliate against whistleblowers in any way. If you are involved in such conduct you may be subject to disciplinary action.

Whistleblowers must not suffer any unfair or detrimental treatment as a result of raising a genuine concern.

2020 INVESTIGATION & TERMINATION

In 2020, NSO also investigated and substantiated an instance of product misuse to target a protected induvial. Following the investigation process, which included discussions with the former customer, extensive data review, and a final determination by the GRCC, NSO terminated the use of Pegasus.

In the past year, we opened 12 investigations of product misuse.

iii. Investigation of Potential Product Misuse Procedure

NSO implemented its Product Misuse Investigations Procedure ("Product Misuse Procedure"), adopted in April 2020, to provide a framework for responding to reports of potential product misuse. The Product Misuse Procedure provides guidance to facilitate the timely investigation of potential product misuse, and for consistent and swift mitigation measures to be taken when appropriate. The Product Misuse Procedure also governs the process for conducting investigations into alleged misuse, including a thorough review of potential human rights abuses.

The Product Misuse Procedure provides guidance to facilitate the timely investigation of potential product misuse and that consistent and swift mitigation measures are taken when appropriate.

NSO's policy ensures that each investigation is conducted in accordance with a number of investigative goals, including to:

- Comply with applicable laws and NSO policies, including the HR Policy,
- Respect the rights of all stakeholders,
- Determine key facts and causes,
- Perform investigations objectively and expeditiously,
- Draw appropriate conclusions, balancing the rights of stakeholders,
- Undertake appropriate remedial action, if any, and
- Preserve confidentiality of the incident reporter to avoid or minimize retaliation, if applicable.

Upon receipt of information about a potential misuse, the Company undertakes, in all cases, a preliminary review to determine whether there is sufficient information to appropriately investigate a potential instance of product misuse, including whether the allegation is technically feasible. The Vice President for Compliance also responds to the whistleblower, seeks any additional information necessary to conduct a preliminary review and any related investigation, and takes all necessary steps to avoid or minimize the risk of any retaliation against the reporter. The Vice President for Compliance coordinates with the Management Committee to determine how to proceed.

Following the preliminary review, the Management Committee appoints the investigation team, led by an attorney, if the determination is to proceed with a full investigation. Investigations may include review of data, interviews, meetings, and evaluation of objective risk factors, including an analysis of whether the customer has engaged in previous human rights abuses. NSO Compliance will evaluate information from the customer, such as information about the process followed in connection with use of NSO products to target specific individuals, the duration of use, circumstances leading an individual to believe they were targeted using an NSO product, and customer country information. The customer is contractually required to provide this information which is maintained in the customer's systems logs in a tamper proof manner. Refusal to cooperate shall lead to immediate suspension of the customer's right to use the system. The Compliance Team will also engage in an in-depth review of media reports, open source research, analysis of domestic law and protections, customer processes, and adherence to international human rights norms. This analysis will include a review of the legal basis for the customer's use of NSO's products, their interfering with individual human rights at issue and whether the customer applied sufficient safeguards when obtaining intelligence using NSO products.

During an investigation, NSO's Compliance Team meets directly with the customer to seek and understand customer compliance with the terms of the agreement; customer practices regarding compliance with the legal framework, operational protections, the customer reporting lines, responses to previous human rights abuses, if any, and the basis for interception.

Investigation results are shared with the Management Committee and the GRCC to collaboratively determine next steps and potential remediation. Depending on the outcome of the investigation, when warranted, the Company will take appropriate corrective action to mitigate potential harm. As a result of the findings, the customer may be subject to corrective action ranging from retraining to termination of the relationship.

In some cases, we are unable to conclusively determine whether there was or was not a misuse of our products. In those instances, we develop and implement additional mitigation measures designed to prevent future misuse.

Through our experience conducting these investigations, and with recommendations from our external advisors, NSO has strengthened our initial due diligence and review processes, including by enhancing the initial assessment of domestic laws, strengthening contractual provisions, and providing human rights training for customer personnel.

However, a number of inherent challenges remain given the nature of our customers. Because of the strict confidentiality requirements of our customers, we are unable to provide actual or alleged victims with information about adverse impacts or implemented remediation, or even acknowledge relationships with specific customers. Even where we identify product misuse, we cannot breach these confidentiality requirements. While we cooperate with states to try to ensure that when abuses occur within their jurisdictions those affected have access to effective remedy, the confidentiality restrictions limit our ability to do much more. While we do follow the approaches described in the UNGPs to the extent feasible with respect to remediation, we and the UNGPs recognize this is a complex and difficult area in particular for our sector. We have received a range of suggestions from stakeholders to enhance our transparency in this respect despite our confidentiality limitations, and how we may more effectively contribute to remedies for affected individuals. In 2021, we aim to begin at least testing, if not implementing, some of these suggestions.

Implementation of relevant policies and procedures

Dissemination of policies/procedures

NSO's HR Policy and the Internal Whistleblowing Policy are available on the Company intranet and website, and are shared with all new Company employees when hired. In addition, the External Whistleblowing Policy is available on NSO's website. NSO's HRDD Procedure and Product Misuse Procedure are posted on the Company's Compliance portal and made available to all employees involved in either the due diligence or product misuse investigation processes.

Training and communications

In 2020, out of the twelve reports raised through our external and internal whistleblowing processes:

- NSO conducted five investigations into product misuse on four continents, with the guidance of external advisors. Of the five:
  - One case resulted in termination of NSO's relationship with the End Customer.
  - Two resulted in the required implementation of additional mitigation measures.
  - Two are still being reviewed.

- For the remaining seven reports, following our preliminary review, we could not identify sufficient information to conduct investigations despite our efforts or the report clearly was not related to the use of our system.

NSO has conducted human rights trainings for employees. All new employees receive human rights training as part of their on-boarding process. In addition, the Company trains existing employees in key functions, (including sales, marketing, and those with direct relationships with clients), regarding human rights twice a year, along with regular employee updates regarding human rights. The Vice President for Compliance also meets regularly with the Company's R&D team to discuss human rights concerns, mitigating measures, and relevant questions, and each new product is evaluated from a human rights lens. In 2020, the Company, with support from human rights advisors, conducted approximately 18 targeted trainings focusing specifically on human rights. Some 121 participants were in attendance for these targeted training sessions. Finally, our CEO includes human rights concerns in nearly all of his "all hands" meetings. Our trainings also incorporate learnings from investigations and application of our human rights framework.

NSO has conducted human rights trainings for employees… NSO also provides comprehensive human rights training to customers.

NSO also provides comprehensive human rights training to customers. This training includes a discussion of human rights obligations, the international framework for human rights norms, and customer responsibilities with respect to individual human rights. Training sessions include discussion of the fundamental human rights of individuals, focusing on the right to privacy and the right to freedom of expression. Key stakeholders are required to attend. Through the course of 2020, approximately 127 customer participants attended the 18 human rights trainings held by NSO.

6. Government Oversight

Even after we have completed our internal human rights processes, we are closely regulated by export control authorities in the countries from which we export our products: Israel, Bulgaria and Cyprus. The

Defense Export Controls Agency ("DECA") of the Israeli Ministry of Defense strictly restricts the licensing of Pegasus, conducting its own analysis of potential customers from a human rights perspective. While we have endeavored to create a robust internal framework to prevent misuse, we also are subject to an "in depth" regulatory review. Moreover, DECA has, in fact, in quite a few cases, denied our applications for export licenses.

We are proud to be the first company in the cyber industry that is implementing policies towards complete alignment with the UNGPs

7. Looking Ahead

In the coming year, as we strive to further strengthen our protection of human rights, we plan to deepen our activities in certain areas, including:

- Conducting a focused impact assessment regarding the potential misuse of our products in connection with the media and journalists;
- Further analyzing recent U.S. guidance[2] and suggested and adopted changes in E.U. export control laws in comparison with our processes;
- Convening roundtables to continue to engage with human rights experts and stakeholders, as well as industry leaders;
- Supporting further development of industry standards, rules and regulations for human rights safeguards;
- Working to devise additional potential measures to protect vulnerable populations from misuses of our products;
- Evaluating potential ways to facilitate remedy for affected individuals, including obtaining constructive input from stakeholders while dealing with confidentiality constraints;
- Working on identifying additional means of monitoring the use of our products beyond what is available today, including further perspectives independent of the company;
- Further developing approaches to increase transparency, despite our inherent constraints.

Through these activities, we believe that we will develop a better understanding of how we can enhance our human rights program, better respect the human rights of those potentially impacted by our products and activities, and further the overall standards put into practice throughout our industry.

We are proud to be the first company in the cyber industry that is implementing policies toward complete alignment with the UNGPs. We will constantly work to improve our policies and practices to further assure that no misuse is committed in the use of our systems, particularly given the absence of best practices and guidance both for states and our industry to appropriately balance human rights and individual liberties with the demands of the fight against major crimes and terrorism.

[2]The U.S. Department of State Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities is available at https://www.state.gov/wp-content/uploads/2020/10/DRL-Industry-Guidance-Project-FINAL-1-pager-508-1.pdf. REGULATION (EU) 2021/821 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items is available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:206:FULL&from=EN

We hope this report helps shed light on our evolving program and we welcome further constructive guidance to respond to the challenges of the technology and human rights nexus.
You are invited to reach our VP, Compliance at chaimg@nsogroup.com

1 – Excerpt of Contracts Provisions

1. The End-User hereby represents and warrants that it and its respective employees and agents: (i) shall fully Appendix and strictly comply with all applicable domestic laws and regulations, including but not limited to those related to surveillance activities, the rights to privacy and freedom of expression as defined by domestic laws and regulations, and obligations to obtain judicial warrants, consents, approvals and/or decrees to the extent required by law for each and every use of the System, (ii) have received and reviewed the NSO Group Human Rights Policy (at https://www.nsogroup.com/wp-content/uploads/2019/09/NSO-Human-Rights-Policy_September19.pdf), and understand the terms, (iii) shall use the System only for the legitimate and lawful prevention and investigation of serious crimes and terrorism, as defined in Exhibit F or in domestic law in a manner substantially similar to Exhibit F, with the definitions in Exhibit F controlling in cases of any material conflict between the definition of such crimes in domestic law and Exhibit F, (iv) shall respect Human Rights and fully and strictly adhere to Human Rights norms at all times in using the System, including the rights to Privacy and Freedom of Expression as contained in the International Covenant of Political and Civil Rights Articles 17 and 19, and not target individuals or groups because of their race, color, sex, language, religion, political or other opinions, national or social origin, property, birth or other status or their otherwise lawful exercise or defense of Human Rights, and (v) will immediately notify the Company of any knowledge it may have regarding a misuse or potential misuse of the System which may result in a violation of Human Rights, may result in a violation of this Agreement, and/or which could cause the Company to be in breach of any of its legal and ethical obligations and/or which could cause the Company commercial or reputational injury.

2. To the extent not otherwise set forth by law, End-User shall formulate and strictly abide by a surveillance procedure or protocol for use of the System. Such procedure shall follow the details set out in the training materials provided to the End User and shall include, at minimum, the provisions regarding the following:
• Legitimate surveillance request supported by evidence; Suspected crimes; Surveillance duration and renewals; Retention period; Approval to be granted in writing by a duly authorized independent oversight authority in accordance with local laws.
3. The End-User hereby represents and warrants that it will promptly investigate any allegations of Human Rights violations allegedly caused by the End-User that are brought to its attention, notify the Company of the results of that investigation and take appropriate remedial action where such investigations confirm Human Rights violations have occurred. The End-User shall have in place a procedure for grievances by third parties through which such third parties can raise complaints

regarding Human Rights matters. The End-User will provide such periodic certificates of compliance with this provision upon request by the Company.

4. End-User agrees that in case of Human Rights violations, appropriate remedial action by the End User may include deletion of data (and all copies whether electronic or physical) obtained through the System, re-training or discipline of End-User employees responsible for misuse, or other measures designed to prevent the recurrence of misuse of the System.

5. Each party shall cooperate with any other party with regard to any inquiry, dispute, or controversy in which the other party may become involved and of which the party may have knowledge. Such cooperation shall include disclosure of relevant documents, such as documents or information related to compliance with the representations made in this Section 18; financial information; and interviews of the party's principals, directors, and key personnel. Such obligation shall continue after the expiration or termination of this Agreement.